

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/019108

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L9/08, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L9/08, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005  
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
JSTPLUS FILE(JOIS), WPI(DIALOG), SOSU, SEISEI (in Japanese)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Generation of RSA Keys That Are Guaranteed to be Unique for Each User, Computer Security, Vol.19, No.3, pages 282 to 288, 2000, particularly, 3. User-Dependent RSA Key Generation	1-23
A	WO 99/52241 A2 (CITIBANK, N.A.), 30 March, 1999 (30.03.99), All pages; particularly, page 5, lines 19 to 30 & AU 9950789 A & EP 1068696 A2 & JP 2002-510810 A & US 6404890 B1 & US 2002/154768 A1 & US 6496929 B2	1-23

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance  
"E" earlier application or patent but published on or after the international filing date  
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other means  
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
"&" document member of the same patent family

Date of the actual completion of the international search  
18 April, 2005 (18.04.05)

Date of mailing of the international search report  
10 May, 2005 (10.05.05)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/019108

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1026851 A1 (Hewlett-Packard Co.), 09 August, 2000 (09.08.00), Particularly, Par. Nos. [0012], [0055] to [0060] (Family: none)	1-23
A	JP 7-121107 A (NEC Corp.), 12 May, 1995 (12.05.95), Particularly, Par. Nos. [0008] to [0019] (Family: none)	1-23
A	Fast Generation of Secure RSA-Moduli with Almost Maximal Diversity, Lecture Notes in Computer Science, Vol.434, pages 636 to 641, 1990, particularly, 2. Theoretical Results on the Decipherability by Multiple Encryption, 3. Recursive Algorithm for Generating Cryptographically Secure Primes and RSA-Moduli with Almost Maximal Diversity	1-23
E, A	US 6687375 B1 (International Business Machines Corp.), 03 February, 2004 (03.02.04), All pages (Family: none)	1-23